Glossario

Modulo Proteggere i dispositivi digitali

ENRICO BASILE

Accesso non autorizzato
Entrare in un sistema o dispositivo senza permesso. È un rischio per la sicurezza e può essere illegale.

Account utente
Profilo personale con credenziali (nome utente e password) per accedere a servizi digitali o computer scolastici.

Antivirus
Software che rileva, blocca e rimuove virus e altri malware dai dispositivi.

Autenticazione
Procedura per verificare l'identità di un utente (es. tramite password, PIN o riconoscimento biometrico) per accedere a un dispositivo o sistema.

Aggiornamento (Update)
Installazione delle versioni più recenti di un software o sistema operativo per correggere errori e aumentare la sicurezza.

Backup
Copia di sicurezza dei dati archiviati su un altro dispositivo o in cloud, utile in caso di guasti o attacchi informatici.

Blocca schermo
Funzione che impedisce l'uso del dispositivo da parte di altri quando ci si allontana. Utile attivarla sempre.

Browser
Programma usato per navigare su Internet (es. Chrome, Firefox). Deve essere aggiornato per evitare rischi di sicurezza.

Cartella condivisa
Spazio digitale accessibile da più utenti. Va gestita con attenzione per evitare accessi indesiderati.

Chiavetta usb (o pen drive)
Supporto rimovibile per salvare e trasferire dati. Può contenere virus: va usata con attenzione.

Cloud
Servizio online che consente di salvare dati su Internet (es. Google Drive). Sicuro se usato con password robuste.

Dispositivo mobile
Strumento elettronico portatile come smartphone o tablet. Anche questi vanno protetti con password e aggiornamenti.

Firewall
Sistema che controlla e limita l'accesso alla rete per proteggere i dispositivi da accessi non autorizzati.

Logout
Uscire da un account o sistema in modo sicuro. Va fatto sempre quando si finisce di usare un dispositivo.

Malware
Programma dannoso (virus, trojan, ransomware) che può infettare un dispositivo digitale e causare danni o perdita di dati.

Password
Parola o codice segreto usato per autenticarsi e proteggere l'accesso a dispositivi o account.

Phishing
Tentativo di truffa via email o messaggi per rubare dati personali o password. Non bisogna mai cliccare su link sospetti.

Responsabile della protezione dei dati (rpd)
Figura prevista dal GDPR che si occupa della sicurezza dei dati personali nella scuola.

Sicurezza informatica (cybersecurity)
Insieme di pratiche, tecnologie e processi per proteggere dispositivi, dati e reti da attacchi o accessi non autorizzati.

Software aggiornato
Programmi e sistemi operativi aggiornati con le ultime patch di sicurezza per correggere vulnerabilità.VPN (VIRTUAL PRIVATE NETWORK): Rete privata virtuale che protegge la connessione internet, rendendo sicuro l'accesso a reti pubbliche.

Wi-fi sicuro
Rete wireless protetta da password e crittografia, per evitare accessi indesiderati.